
HAN ZHENG

BC 156, EPFL, 1015 Lausanne
han.zheng@epfl.ch

EDUCATION

École Polytechnique Fédérale de Lausanne PhD candidate in Computer Science Supervisor: Prof. Mathias Payer	<i>2023 Aug - Now</i>
University of Chinese Academy of Science M.E. in Electronic Information Engineering	<i>2020 Aug - 2023 Jun</i>
Xidian University B.E. in Information Countermeasure Technique	<i>2016 Aug - 2020 Jun</i>

EXPERIENCE

École Polytechnique Fédérale de Lausanne Visiting Student in HexHive. Supervisor: Prof. Mathias Payer	<i>2021 Dec - 2022 Dec</i>
--	----------------------------

PROJECTS

FishFuzz: Catch Deeper Bugs by Throwing Larger Nets Boosting the Multi-Target Directed Greybox Fuzzing by improving the precision of distance calculation and dynamically adjusting target priority. FishFuzz found 38 CVEs in exhaustively tested programs.	<i>USENIX Sec'23</i>
🏆 FishFuzz ('s extension) won 2nd Place in SBFT'24.	

MendelFuzz: The Return of the Deterministic Stage Analyzing the key limitation of the deterministic stage in Coverage-Guided Greybox Fuzzing, further improves the deterministic stage by skipping redundant mutations. The new deterministic stage become default mode in AFL++.	<i>FSE'25</i>
🏆 MendelFuzz became the default mode in AFL++.	

Squeezing Juicy Variant Bugs Out Of Modern Browsers Formalizing the bug variant analysis with a standardized model, covering both memory safety and logical vulnerabilities. Grape receives five CVEs from Chrome and one CVE from Microsoft.	<i>WOOT'26</i>
🏆 Grape received 17,500 USD bounty from Google.	

AWARDS AND SCHOLARSHIPS

Chrome Vulnerability Reward Program (2025) , 8,000 USD, Google	<i>2026 Jan</i>
Google Cloud Research Credit , 500 CHF, Google	<i>2025 Jun</i>
Chrome Vulnerability Reward Program (2024) , 25,000 USD, Google	<i>2025 Jan</i>
SBFT FuzzBench Competition 2nd Place , 300 EUR, Google	<i>2024 Apr</i>
EDIC PhD Fellowship , 54,000 CHF, EPFL	<i>2023 Sep</i>
IC Master Scholarship , 22,400 CHF, EPFL	<i>2021 Dec</i>
Visiting Scholarship , 23,400 CHF, China Scholarship Council	<i>2021 Dec</i>

BUG HUNTING

Google Leaderboard Ranking: #42 in Google VRP 2024

VSCode: CVE-2025-32726 (AzureDataStudio, High)

ChromeOS: CVE-2025-2509 (Virglrenderer, Medium)

Chrome: b/467297219 (Blink, High), CVE-2025-0438 (Tracing, High), CVE-2025-0436 (Skia, High), b/365802556 (Blink, High), CVE-2024-7968 (UI, High), b/349253666 (UI, Medium), CVE-2024-5846 (PDF, Medium), CVE-2024-5847 (PDF, Medium), CVE-2024-7018 (PDF, Medium)

WebRTC (not impacting Chrome): b/371686447 (WebRTC, High), b/371615496 (libyuv, Medium)

Wireshark: CVE-2024-0209, CVE-2024-0210

iOS / MacOS: CVE-2022-26981 (Font, High)

SERVICE

Technical Program Committee: ASE'26, ISSTA'26, FUZZING'26, ASE'25, FUZZING'25

Journal Reviewer: TSE, TOSEM, TIFS

Shadow TPC: NDSS'24, ISSTA'24

SKILLS

Coding: C, Python, GDB, LLVM, AFL/AFL++, Docker

Languages: Chinese (Mother Tongue), English (IELTS 7.0)

SUPERVISE / MENTOR

Zurab Tsinadze, Master@EPFL, Master thesis.

2025 Jan - 2025 Jun

Zezhong Ren, PhD@UCAS, PhD project.

2024 Aug - 2025 Aug

Wenhao Fang, Bachelor@St.Andrews, Summer@EPFL project.

2026 Jan - Now

TEACHING

MAN, Le cours de mise à niveau, (24 Spring)

Teaching Assistant

COM-402, Information Security and Privacy, (24 Fall, 25 Fall)

Teaching Assistant

CS-412, Software Security, (25 Spring)

Teaching Assistant

INVITED TALKS

Research Seminar at HKUST, Hong Kong Hosted by Prof. Dongdong She

2025 July

Research Seminar at Tsinghua University, Beijing Hosted by Prof. Chao Zhang

2025 July

ESEC/FSE'25, Trondheim MendelFuzz presentation

2025 June

SBFT24@ICSE, Lisbon FuzzBench competition report

2024 Apr

Research Seminar at HUST, Wuhan Hosted by Prof. Wei Zhou

2023 June

PUBLICATIONS

[6] **Han Zheng**, Flavio Toffalini, Qiang Liu, and Mathias Payer. Squeezing juicy variant bugs out of modern browsers. In *20th USENIX WOOT Conference on Offensive Technologies (WOOT 26)*, 2026

[5] Zezhong Ren, **Han Zheng**, Zhiyao Feng, Qinying Wang, Marcel Busch, Yuqing Zhang, Chao Zhang, and Mathias Payer. Sysyphuzz and the pressure of more coverage. In *33rd Annual Network and Distributed System Security Symposium, NDSS*, 2026

[4] **Han Zheng**, Flavio Toffalini, Marcel Böhme, and Mathias Payer. Mendelfuzz: The return of the deterministic stage. *Proceedings of the ACM on Software Engineering*, 2(FSE):44–64, 2025

[3] **Han Zheng**, Flavio Toffalini, and Mathias Payer. Tunefuzz: Adaptively exploring target programs. In *Proceedings of the 17th ACM/IEEE International Workshop on Search-Based and Fuzz Testing*, pages 61–62, 2024

-
- [2] **Han Zheng**, Jiayuan Zhang, Yuhang Huang, Zezhong Ren, He Wang, Chunjie Cao, Yuqing Zhang, Flavio Toffalini, and Mathias Payer. {FISHFUZZ}: Catch deeper bugs by throwing larger nets. In *32nd USENIX Security Symposium (USENIX Security 23)*, pages 1343–1360, 2023
 - [1] Zezhong Ren, **Han Zheng**, Jiayuan Zhang, Wenjie Wang, Tao Feng, He Wang, and Yuqing Zhang. A review of fuzzing techniques. 2021